National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314

14 March 2018

Report Number: CCEVS-VR-PP-0042
Dated: 14 March 2018
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Cygnacom Solutions, Inc. Common Criteria Testing Laboratory
McLean, Virginia

Gossamer Security Solutions Common Criteria Testing Laboratory
Catonsville, Maryland

Acumen Security Common Criteria Testing Laboratory
Rockville, Maryland

Table of Contents

Table of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the collaborative Protection Profile for Network Devices, Version 2.0 (NDcPP20), also referred to as the Network Devices collaborative Protection Profile (NDcPP). It presents a summary of the NDcPP and the evaluation results.

The evaluation of the NDcPP was performed concurrent with the first five product evaluation against the cPP's requirements. In this case the Target of Evaluations (TOEs) were the:

1. Extreme Networks Summit Series Switches EXOS v22.3 family of network devices, performed by CygnaCom Solutions Inc. in McLean, Virginia, United States of America.
2. Brocade FastIron Switch/Router 8.0.70, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.
3. Brocade FastIron ICX Series Switch/Router 08.0.70, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.
4. Cisco Catalyst 6500 and 6807-XL Series Switches with Sup2T and Sup6T running IOS 15.5SY, performed by Acumen Security in Rockville, MD, United States of America.
5. McAfee ATD v4.0, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

These evaluations addressed the base requirements of the NDcPP, as well as a few of the additional requirements contained in Appendices A and B.

An additional review of the cPP was performed independently by the Validation Report (VR) author as part of the completion of this VR, to confirm that it meets the claimed APE assurance requirements.

The evaluation determined that the NDcPP is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this VR has been evaluated at NIAP approved CCTLs using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the NDcPP, the majority of the ASE work units served to satisfy the APE work units as well.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The initial results by the validation team found that the evaluation showed that the NDcPP did not meet the requirements of the APE components. These findings were confirmed by the VR author and NIAP. NIAP notified the Network Device international Technical Community (ND iTC) of all noted deficiencies. The ND iTC updated the cPP and determined the impact of the changes were typographical errors related to the conventions for indicating

assignments and selections and did not affect the security functionality of the PP. Subsequently, the ND iTC corrected all deficiencies and published the NDcPP 2.0 + Errata 20180314. NIAP reviewed the Errata and confirmed all changes were made. As a result, the validation team found that the evaluation showed that the NDcPP 2.0 + Errata 20180314 meets the requirements of the APE components. Since the Errata changes had no impact on the security functionality, all five products are compliant.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against cPPs that contain Assurance Activities, which are interpretations of CEM work units specific to the technology described by the cPP.

In order to promote thoroughness and efficiency, the evaluation of the NDcPP was performed concurrent with the first five product evaluation against the cPP's requirements. In this case the Target of Evaluations (TOEs) were the:

1. Extreme Networks Summit Series Switches EXOS v22.3 family of network devices, performed by CygnaCom Solutions Inc. in McLean, Virginia, United States of America;
2. Brocade FastIron Switch/Router 8.0.70, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America;
3. Brocade FastIron ICX Series Switch/Router 08.0.70, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America; and
4. Cisco Catalyst 6500 and 6807-XL Series Switches with Sup2T and Sup6T running IOS 15.5SY, performed by Acumen Security in Rockville, MD, United States of America.
5. McAfee ATD v4.0, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America;

These evaluations addressed the base requirements of the NDcPP, as well as a few of the additional requirements contained in Appendices A and B.

The NDcPP contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional" and "Selection-based" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

Because these discretionary requirements may not be included in a particular ST, the initial use of the cPP will address (in terms of the cPP evaluation) the base requirements as well as

any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the NDcPP that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made when that occurs.

The following identifies the cPP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this cPP and any subsequent evaluations that address additional optional and/or selection-based requirements in the NDcPP.

Protection Profiles	Collaborative Protection Profile for Network Devices, Version 2.0, 5 May 2017
	Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
ST (Base)	Extreme Networks Summit Series Switches Security Target, Version 2.4, 19 December 2017
	Brocade Communication Systems, Inc., Brocade FastIron Switch/Router (NDcPP20/VPNGWEP21) Security Target, Version 0.6, 13 February 2018
	Brocade Communication Systems, Inc., Brocade FastIron Switch/Router 8.0.70 (NDcPP20) Security Target, Version 0.4, 31 January 2018
	Cisco Catalyst 6500 and 6807-XL Series Switches running IOS 15.5SY Common Criteria Security Target, Version 1.0, 19 January 2018
	McAfee, Inc. Advanced Threat Defense running software version 4.0.2 (NDcPP20) Security Target, Version 0.7, 06 March 2018
Assurance Activity Report (Base)	NDcPP v2.0 Assurance Activity Report for Extreme Networks Summit Series Switches running EXOS v22.3, Version 0.9, 20 December 2017
	Assurance Activity Report (NDcPP20) for Brocade Communications Systems, Inc.FastIron Switch/Router 8.0.70, Version 0.3, 13 February 2018.
	Assurance Activity Report (NDcPP20/VPNGWEP21) for Brocade FastIron ICX Series Switch/Router 08.0.70, Version 3.0, 13 February 2018.
	Assurance Activity Report for Cisco Catalyst 6500 and 6807-XL series Switches, version 15.5SY, Version 1.1, 17 January 2018.
	Assurance Activity Report (NDcPP20) for McAfee, Inc. Advanced Threat Defense running software version 4.0.2, Version 0.3, 03 March 2018.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	CygnaCom Solutions, Inc., McLean, VA, USA Gossamer Security Solutions, Catonsville, MD, USA
	Acumen Security, Rockville, MD, USA

3 NDcPP Description

The NDcPP specifies information security requirements for network devices, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A network device in the context of the cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfill the requirements of the cPP.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained,

Assumption Name	Assumption Definition
	following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly

Threat Name	Threat Definition
	designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTI VITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_ FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

Threat Name	Threat Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOESecurity Objective Definition
There are no listed security objectives for the TOE. .	

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 Requirements

As indicated above, requirements in the NDcPP are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the Extreme Networks Summit Series Switches evaluation activity referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FAU_GEN.2: User Identity Association	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FAU_STG_EXT.1: Protected Audit Event Storage	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_CKM.2: Cryptographic Key Establishment	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_CKM.4: Cryptographic Key Destruction	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series Switches
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_RBG_EXT.1: Random Bit Generation	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_AFL.1: Authentication Failure Management	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron,

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication		Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_PMG_EXT.1: Password Management	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_UIA_EXT.1: User Identification and Authentication	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_UAU_EXT.2: Password-based Authentication Mechanism	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_UAU.7: Protected Authentication Feedback	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FMT_MTD.1/CoreData: Management of TSF Data	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FMT_SMF.1: Specification of Management Functions	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FMT_SMR.2: Restrictions on Security Roles	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FPT: Protection of the TSF	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FPT_APW_EXT.1: Protection of Administrator Passwords	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FPT_TST_EXT.1: TSF Testing	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FPT_TUD_EXT.1: Trusted Update	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FPT_STM_EXT.1: Reliable Time Stamps	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron,

Requirement Class	Requirement Component	Verified By
		Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FTA_SSL.3: TSF-initiated Termination	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FTA_SSL.4: User-initiated Termination	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FTA_TAB.1: Default TOE Access Banners	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FTP_TRP.1/Admin: Trusted Path	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected audit trail storage	PP Evaluation
	FAU_STG_EXT.2/LocSpace: Counting lost audit data	PP Evaluation
	FAU_STG.3/LocSpace: Action in case of possible audit data loss	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certificate Validation	PP Evaluation
FMT: Security Management	FMT_MOF.1/Services: Management of security functions behavior	Brocade FastIron ICX
	FMT_MTD.1/CryptoKeys: Management of TSF data	Cisco Catalyst 6500 and 6807-XL Series.
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection	PP Evaluation
FTP: Trusted Path/Channels	FTP_TRP.1/Join: Trusted Path	PP Evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLSC_EXT.1: DTLS Client Protocol	PP Evaluation
	FCS_DTLSC_EXT.2: DTLS Client Protocol – with authentication	PP Evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol	PP Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Protocol with mutual authentication	PP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	PP Evaluation
	FCS_IPSEC_EXT.1: IPsec Protocol	Brocade FastIron ICX & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_SSHC_EXT.1: SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	Extreme Networks Summit Series, Brocade FastIron, & Cisco Catalyst 6500 and 6807-XL Series.
	FCS_TLSC_EXT.1: TLS Client Protocol	McAfee ATD & Brocade FastIron
	FCS_TLSC_EXT.2: TLS Client Protocol with authentication	Extreme Networks Summit Series Switches Security Target
	FCS_TLSS_EXT.1: TLS Server Protocol	McAfee ATD
	FCS_TLSS_EXT.2: TLS Server Protocol with mutual authentication	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_X509_EXT.2: X.509 Certificate Authentication	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	FIA_X509_EXT.3: X.509 Certificate Requests	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
FPT: Protection of the TSF	FPT_TST_EXT.2: Self-tests based on certificates	Brocade FastIron ICX
	FPT_TUD_EXT.2: Trusted Update based on certificates	PP Evaluation
FMT: Security Management	FMT_MOF.1/AutoUpdate: Management of security functions behaviour	PP Evaluation
	FMT_MOF.1/Functions: Management of security functions behaviour	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the NDcPP.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_ECD.1: Extended Components Definition	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_INT.1: ST Introduction	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_OBJ.1: Security Objectives for the Operational Environment	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_REQ.1: Stated Security Requirements	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_SPD.1: Security Problem Definition	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ASE_TSS.1: TOE Summary Specification	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
ADV: Development	ADV_FSP.1 Basic Functional Specification	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	AGD_PRE.1: Preparative Procedures	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
	ALC_CMS.1: TOE CM Coverage	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
ATE: Tests	ATE_IND.1: Independent Testing - conformance	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron,

Requirement Class	Requirement Component	Verified By
		Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.

7 Results of the Evaluation

Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
APE_ECD.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
APE_INT.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
APE_OBJ.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
APE_REQ.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.
APE_SPD.1	Pass	Extreme Networks Summit Series, McAfee ATD, Brocade FastIron, Brocade FastIron ICX, & Cisco Catalyst 6500 and 6807-XL Series.

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance

in the NDcPP Assurance Activities to determine whether or not the claims made are justified.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] *Extreme Networks Summit Series Switches Security Target*, Version 2.4, 19 December 2017.

[7] *NDcPP v2.0 Assurance Activity Report for Extreme Networks Summit Series Switches running EXOS v22.3*, Version 0.9, 20 December 2017.

[8] Brocade Communication Systems, Inc., Brocade FastIron Switch/Router (NDcPP20/VPNGWEP21) Security Target, Version 0.6, 13 February 2018

[9] Assurance Activity Report (NDcPP20) for Brocade Communications Systems, Inc.FastIron Switch/Router 8.0.70, Version 0.3, 13 February 2018.

[10] Brocade Communication Systems, Inc., Brocade FastIron Switch/Router 8.0.70 (NDcPP20) Security Target, Version 0.4, 31 January 2018

[11] Assurance Activity Report (NDcPP20/VPNGWEP21) for Brocade FastIron ICX Series Switch/Router 08.0.70, Version 3.0, 13 February 2018.

[12] Cisco Catalyst 6500 and 6807-XL Series Switches running IOS 15.5SY Common Criteria Security Target, Version 1.0, 19 January 2018.

[13] Assurance Activity Report for Cisco Catalyst 6500 and 6807-XL series Switches, version 15.5SY, Version 1.1, 17 January 2018.

[14] McAfee, Inc. Advanced Threat Defense running software version 4.0.2 (NDcPP20) Security Target, Version 0.7, 06 March 2018

[15] Assurance Activity Report (NDcPP20) for McAfee, Inc. Advanced Threat Defense running software version 4.0.2, Version 0.3, 03 March 2018.

[16] *collaborative Protection Profile for Network Devices*, Version 2.0, 5 May 2017.

[17] *collaborative Protection Profile for Network Devices*, Version 2.0 + Errata 20180314, 14 March 2018.